UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/930,784 | 08/15/2001 | William M. Gillon | 50588/360 | 2550 |

32641 7590 03/04/2008

DIGEO, INC C/O STOEL RIVES LLP
201 SOUTH MAIN STREET, SUITE 1100
ONE UTAH CENTER
SALT LAKE CITY, UT 84111

| EXAMINER | |
|---|---|
| KHOSHNOODI, NADIA | |
| ART UNIT | PAPER NUMBER |
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 03/04/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/930,784 | GILLON ET AL. | |
| | Examiner | Art Unit | |
| | NADIA KHOSHNOODI | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5,11-21 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 11-21 and 23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/10-31-2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/31/2007 has been entered.

### *Response to Amendment*

Claims 6-10 and 22 are cancelled. Applicant's arguments/amendments with respect to amended claims 1-3, 11-13, 17-19, 21, & 23 and previously presented claims 4-5, 14-16, & 20 filed 10/31/2007 have been fully considered and therefore the claims are rejected under new grounds.

### *Claim Rejections - 35 USC § 103*

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 3-5, 11-12, and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards, US Patent No. 6,690,795, and further in view of Peacock, "Features

and Utilization of Motorola's Advanced INFOSEC Machine, AIM, in Embedded Encryption Applications."

As per claim 1:

Richards substantially teaches a computer-implemented method comprising: encrypting a group of original multimedia channel keys using a first encryption format decryptable by a first multimedia receiver to produce a first group of encrypted multimedia channel keys (col. 16, line 46 – col. 17, line 13 and col. 17, line 44 – col. 18, line 4); encrypting said same group of original multimedia channel keys using a second encryption format decryptable by the second multimedia receiver to produce a second group of encrypted multimedia channel keys, the second encryption format being developed after the first encryption format (col. 16, line 46 – col. 17, line 13 and col. 17, line 44 – col. 18, line 4), and concurrently transmitting said first group of encrypted multimedia channel keys to a plurality of multimedia subscribers having either the first multimedia receiver or the second multimedia receiver, wherein said first group of encrypted multimedia channel keys is decryptable by the first multimedia receiver and said second group of encrypted multimedia channel keys is decryptable by the second multimedia receiver but not the first multimedia receiver (col. 16, line 46 – col. 17, line 13 and col. 17, line 44 – col. 18, line 4).

Not explicitly disclosed is the second multimedia receiver being developed after the first multimedia receiver and wherein the encryption format is an encryption algorithm. However, Peacock teaches that replacing legacy systems with new systems, to implement a change from older encryption algorithms to newer encryption algorithms (see Abstract and page 423, col. 2). Peacock further teaches that during the transition phase the chip disclosed is capable of executing

both the first and second encryption algorithm (page 425, col. 2 "The Crypto Processors"). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards to incorporate this seamless migration of analog to digital receivers within a system that also changes the encryption algorithm for multimedia channel keys from an older encryption algorithm to a newer encryption algorithm. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Peacock suggests that using the AIM chip legacy systems using older encryption algorithms can be replaced with newer systems using a newer encryption algorithm without disrupting the service since this chip can be programmed to execute both the new and the old algorithms on page 429, col. 2, "Legacy Replacement/Transition."

As per claim 3:

Richards and Peacock substantially teach the method as in claim 1. Furthermore, Richards teaches the method further comprising: transmitting entitlement information with said group of multimedia channel keys encrypted using said second encryption algorithm, said entitlement information indicating which of said multimedia channels a user has the right to decrypt (col. 18, lines 26-40).

As per claim 4:

Richards and Peacock substantially teach the method as in claim 3. Furthermore, Richards teaches the method further comprising: decrypting said second group of encrypted multimedia channel keys at a multimedia receiver (col. 7, lines 1-14).

As per claim 5:

Richards and Peacock substantially teach the method as in claim 4. Furthermore, Richards teaches the method further comprising: searching said entitlement information to determine whether said user has the right to view a particular channel selected by said user; and decrypting said channel using one of said decrypted keys if said user has said right (col. 18, lines 19-40).

As per claim 11:

Richards substantially teaches a system for comprising: a computer readable storage medium having stored thereon original decryption keys for decrypting said multimedia channels, wherein each original decryption key is successively encrypted in both a first encryption format and a second encryption format to produce first and second encrypted decryption keys, respectively, the second encryption format being developed after the first encryption format (col. 16, line 46 – col. 17, line 13 and col. 17, line 44 – col. 18, line 4); said decryption keys encrypted in said first encryption format being decryptable by the first multimedia receiver (col. 16, line 46 – col. 17, line 13); and said decryption keys encrypted in said second encryption format being decryptable by the second multimedia receiver but not the first multimedia receiver (col. 16, line 46 – col. 17, line 13).

Not explicitly disclosed is the second multimedia receiver being developed after the first multimedia receiver and wherein the encryption format is an encryption algorithm. However, Peacock teaches that replacing legacy systems with new systems, to implement a change from older encryption algorithms to newer encryption algorithms (see Abstract and page 423, col. 2). Peacock further teaches that during the transition phase the chip disclosed is capable of executing both the first and second encryption algorithm (page 425, col. 2 "The Crypto Processors").

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards to incorporate this seamless migration of analog to digital receivers within a system that also changes the encryption algorithm for multimedia channel keys from an older encryption algorithm to a newer encryption algorithm. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Peacock suggests that using the AIM chip legacy systems using older encryption algorithms can be replaced with newer systems using a newer encryption algorithm without disrupting the service since this chip can be programmed to execute both the new and the old algorithms on page 429, col. 2, "Legacy Replacement/Transition."

As per claim 12:

Richards and Peacock substantially teach the system as in claim 11. Furthermore, Richards teaches wherein said second encryption algorithm permits all of said keys to be decrypted in real-time as they are received by said multimedia receiver (col. 20, lines 34-41).

As per claim 14:

Richards and Peacock substantially teach the system as in claim 11. Furthermore, Richards teaches the system further comprising: transmitting entitlement information indicating which of said multimedia channels a user has a right to view (col. 18, lines 26-40).

As per claim 15:

Richards and Peacock substantially teach the system as in claim 14. Furthermore, Richards teaches the system further comprising: said second type of multimedia receiver decrypting only those keys identified by said entitlement information (col. 7, lines 1-14).

As per claim 16:

Richards and Peacock substantially teach the system as in claim 14. Furthermore, Richards teaches the system further comprising: said second type of multimedia receiver being configured to decrypt said decryption keys and using said decryption keys to decrypt multimedia channels identified by said entitlement information (col. 7, lines 1-14).

III. Claims 2, 13, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards, US Patent No. 6,690,795 and "Features and Utilization of Motorola's Advanced INFOSEC Machine, AIM, in Embedded Encryption Applications", as applied to claims 1 and 11-12 above, and further in view of Colligan et al. US Patent No. 6,415,031.

As per claim 2:

Richards and Peacock substantially teach the method as in claim 1. Not explicitly disclosed the method wherein said second encryption algorithm is digital video broadcasting ("DVB") encryption. However, Colligan et al. teach that the encryption algorithm can be DVB encryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards for the second encryption algorithm to be DVB encryption as used with the subscribers' customer keys to yield encrypted channel keys. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Colligan et al. teach that DVB encryption may be used where the DVB standard allows simultaneous encryption of a channel for more than one subscriber station in order to protect various forms of digital content in col. 8, lines 29-41.

As per claim 13:

Richards and Peacock substantially teach the method as in claim 12. Not explicitly disclosed the method wherein said second type of encryption is digital video broadcasting ("DVB") encryption. However, Colligan et al. teach that the encryption algorithm can be DVB encryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards for the second encryption algorithm to be DVB encryption as used with the subscribers' customer keys to yield encrypted channel keys. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Colligan et al. teach that DVB encryption may be used where the DVB standard allows simultaneous encryption of a channel for more than one subscriber station in order to protect various forms of digital content in col. 8, lines 29-41.

As per claim 17:

Richards and Peacock substantially teach the system as in claim 11. Furthermore, Richards teaches the system further comprising: said second multimedia receiver being configured to decrypt a decryption key and use the decryption key to decrypt a multimedia channel (col. 7, lines 1-14).

Not explicitly disclosed is said second multimedia receiver further being configured to re-encrypt said multimedia channel using an alternative encryption algorithm not decryptable by said first multimedia receiver. However, Colligan et al. teach re-encrypting the multimedia channels when received at a remote server in order to store the content in a secure encrypted algorithm using a different key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards to re-encrypt the

multimedia channels using an alternative encryption technique in order to copy protect the content before storing it. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Colligan et al. suggest that storing the digital content in a re-encrypted form by using another key, once the digital content has been received/decrypted from a different source, allows for securely storing the content at a remote server in col. 5, lines 38-40 and col. 6, lines 5-13.

As per claim 18:

Richards, Peacock, and Colligan et al. substantially teach the method as in claim 17. Furthermore, Colligan et al. teach the method wherein said second type of encryption is digital video broadcasting ("DVB") encryption (col. 8, lines 29-41).

As per claim 19:

Richards, Peacock, and Colligan et al. substantially teach the method as in claim 17. Furthermore, Colligan et al. teach the system wherein the first and second multimedia receivers are configured to store said multimedia channels in said alternative encryption algorithm on a mass storage device (col. 6, lines 31-35).

As per claim 20:

Richards, Peacock, and Colligan et al. substantially teach the method as in claim 19. Furthermore, Colligan et al. teach the method wherein the first and second multimedia receivers are configured to decrypt and play back said multimedia channel from said mass storage device responsive to a user request to play back said multimedia channel (col. 6, lines 36-51).

IV. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Richards, US Patent No. 6,690,795 and further in view of Basawapatna et al., US Patent No. 6,598,231 and that which is commonly known in the prior art.

As per claim 21:

Richards substantially teaches a method comprising: encrypting a channel key using one encryption algorithm decryptable by the multimedia receiver to generate a first encrypted channel key (col. 16, line 46 – col. 17, line 13); encrypting said channel key using a second encryption algorithm decryptable by the multimedia receiver to provide a second encrypted channel key (col. 16, line 46 – col. 17, line 13); concurrently transmitting the first and second encrypted channel keys to multimedia receivers, respectively (col. 16, line 46 – col. 17, line 13); transmitting an encrypted channel to the multimedia receivers (col. 16, line 46 – col. 17, line 13); within the first multimedia receiver: decrypting the first encrypted channel key using a first decryption algorithm to recover the channel key (col. 16, line 46 – col. 17, line 13); and decrypting the encrypted channel using the channel key (col. 17, line 44 – col. 18, line 4); and within the second multimedia receiver: decrypting the second encrypted channel key using a second decryption to recover the channel key (col. 16, line 46 – col. 17, line 13); and decrypting the encrypted channel using the channel key (col. 17, line 44 – col. 18, line 4).

Not explicitly disclosed is wherein the first encryption format is a standard encryption algorithm and wherein the second encryption format is a non-standard encryption algorithm. However, Basawapatna et al. teach that the type of encryption chosen is based upon whether the signal is analog or digital. These formats determine whether a standard encryption algorithm would be used, for an analog signal, or if a non-standard encryption algorithm is to be used, for a

digital signal (col. 10, lines 22-31). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards to use a standard encryption algorithm if an analog signal is used and a non-standard encryption algorithm for digital signals (including where the channels are high definition channels). This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Basawapatna et al. suggest that the encryption algorithm is based on whether the signal is analog or digital in col. 7, lines 3-7 and col. 12, lines 31-36.

Also not explicitly disclosed is where there are two different types of multimedia receivers and where the second receiver, not the first, is able to decrypt the channel keys encrypted with a non-standard encryption algorithm. However, Examiner takes official notice that it is commonly known and widely practiced to have analog receivers and digital receivers as two different types of receivers where, as Basawapatna et al. disclosed (shown above) that the encryption algorithm supported will be based on whether the receiver is digital or analog. Thus, it would be obvious to a person skilled in the art to have two different receivers accepting each of the two different signals, namely analog and digital, in order to modify the combination of Richards and Basawapatna et al. in order to save time from converting one signal to another (if there was only one type of receiver).

V. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Richards, US Patent No. 6,690,795; Basawapatna et al., US Patent No. 6,598,231; and that which is commonly known in the prior art, as applied to claim 21 above, and further in view of Colligan et al. US Patent No. 6,415,031.

As per claim 23:

Richards, Basawapatna et al., and that which is commonly known in the prior art substantially teach the method as in claim 21. Not explicitly disclosed the method wherein the non-standard encryption algorithm comprises open encryption. However, Colligan et al. teach that the encryption algorithm can be DVB encryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Richards for the second encryption algorithm to be DVB encryption as used with the subscribers' customer keys to yield encrypted channel keys. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Colligan et al. teach that DVB encryption may be used where the DVB standard allows simultaneous encryption of a channel for more than one subscriber station in order to protect various forms of digital content in col. 8, lines 29-41.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,772,434
2. US Patent No. 5,953,418
3. US Patent No. 5,453,796
4. "Practical Digital Cinema Distribution in an Evolving Technology Environment"
5. "DVB Content Protection and Copy Management - Call for Proposals"

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nadia Khoshnoodi/
Examiner, Art Unit 2137
2/18/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137